Cybersecurity at
MIT Sloan

THE WALL STREET JOURNAL.

JON KRAUSE

Are Boards the Weak Link?

Directors spend a lot more time thinking about cybersecurity. Perhaps they should look in the mirror.

BY JEFFREY PROUDFOOT AND KERI PEARLSON

BOARD MEMBERS are taking on more responsibility for cybersecurity strategy at the companies they oversee. But they might be overlooking one of the organization's biggest vulnerabilities: themselves.

We uncovered this uncomfortable truth while conducting a series of interviews and surveys with dozens of directors across different companies and industries, part of our broader research into boards and cybersecurity issues.

Over the past decade, cybersecurity oversight has become an added board mandate, with directors becoming more accountable for ensuring organizations have robust defenses against attacks in place. That means directors now have access to detailed tactical information about companies' cyber defenses, in addition to other sensitive data.

Despite that, directors haven't traditionally fallen within the scope of most companies' cybersecurity efforts. Nor are most companies we surveyed preparing directors to anticipate, respond to or avoid cyberattacks.

The upshot: The board members themselves, the people responsible for making sure a company is well-protected, could well become the weak link in an organization's cyber defenses.

No preparation

Corporate executives have a number of ways to keep directors abreast of a company's cybersecurity preparedness, including presentations from tech executives, tabletop exercises that simulate hypothetical attacks, and reports on key cybersecurity metrics. However, none of these measures prepare directors to be resilient against potential attacks targeting them directly.

And there's no question that they are uniquely vulnerable. For example, based on research we have done, we know that many board members almost exclusively work remotely, meaning they share a lot of sensitive data electronically. In addition, directors usually aren't involved in, and thus don't benefit from, awareness programs, regular communications and informal water-cooler discussions that help keep cybersecurity on the minds of a company's employees. And since boards may receive cybersecurity status updates only periodically, it can take a while for directors to identify and fully understand emerging threats such as AI-driven cyberattacks and how they might be used to target them individually.

Several board members told us that some directors use public email accounts—rather than official or encrypted messaging systems or document-management platforms—to share board information and communications. One commented that she thought the platform used by the board to share documents for meetings was secure, but she really didn't know for sure.

Other board members said that while they get limited briefings on things like the percentage of employees who fail phishing tests, they have never received training on how to shore up their own personal defenses. Still others reported that, despite a growing focus on cybersecurity, many boards don't have a single director with a cyber background or with formal cybersecurity training.

What can be done?

In light of this risk, what can boards do?

First, the cybersecurity education-and-training programs aimed at rank-and-file employee could be customized for boards.

Second, customized tabletop exercises, in which board members are exposed to a hypothetical cyber incident and asked to respond, could be especially effective in terms of getting board members to recognize and prepare for direct attacks. The immersive nature of a tabletop exercise creates an emotional response that leads participants to become much more invested than they otherwise would in discussions about what to do during a real attack.

Third, organizations might want to include board members in phishing simulations, in which they send fake emails to employees to gauge how many will react and to develop training tools to mitigate the effectiveness of such attacks.

Finally, one-on-one consulting, where security experts are assigned to work with individual directors, might be the most effective training approach. This gives directors the tutoring they need at a time, and in a manner, most suited to them.

Virtually all cybersecurity assets and efforts are focused on protecting the organization itself, but directors need to be included in the security plans, too. If directors are expected to serve as the strategic cybersecurity guards of their companies, more needs to be done to guard the guards.

Jeffrey Proudfoot *is an associate professor at Bentley University and a research affiliate at the Cybersecurity at MIT Sloan (CAMS) research consortium.* ***Keri Pearlson*** *is executive director of CAMS.* ***Stuart Madnick****, founding director of CAMS, contributed to this research. The authors can be reached at* ***reports@wsj.com.***

THIS QR CODE WILL DIRECT YOU TO THE CAMS WEBSITE
https://cams.mit.edu
SCAN ME

THIS QR CODE WILL GIVE YOU ACCESS TO A DIGITAL COPY OF THE ARTICLE
SCAN ME